NEXT COMPUTING

CyberPro Plus 100G

HIGH-SPEED PORTABLE CAPTURE APPLIANCE

The CyberPro Plus 100G is a briefcase-sized portable workstation which offers 10Gbps+ continuous lossless capture, massive storage, and an integrated display for real-time visualization and analysis.

CyberPro appliances are based on a powerful software architecture that offers lossless packet capture, fast query retrieval, IDS alerting and a real-time Threat Hunting / Log Manager. It is integrated into a unique, impossibly small portable form factor, addressing critical elements inherent to a comprehensive incident response plan (IRP). This makes CyberPro ideal for multiple cybersecurity use cases that require onsite response, analysis and mitigation.

The increase of enterprise RTC (real time communication) such as VoIP (voice over IP), along with simple methods of intercepting IP packets, have made RTC a prime target for hackers. This has led to needed response from cybersecurity solution providers to incorporate VoIP features.

CyberPro Plus 100G includes a unique threat-hunting feature: Use a SNORT/ SURICATA rule set for “Retrospective Detection” of PCAP history. Find out if a newly discovered IoC was active in your network – even before the threat was known!

End users, resellers and integrators can incorporate data from any third party threat detection system for a complete cybersecurity solution package.

10Gbps+ continuous lossless packet capture. Configuration options for 4x25G or 2x100G capture interfaces (100Gbps aggregate) continuous PCAP capture only and post analysis / search

20-200 TB storage options via fixed or no-tools removable drives, additional storage up to 200TB

Simultaneous search of PCAP, NetFlow V9 & log files

Up to 50,000 SNORT/SURICATA active IDS rules at line rate

Up to 1 Million active ThreatIP alerts

Active Triggers for user-defined BPF alerts

Threat Hunting: search events, cross-correlate with PCAP, extract key evidence

PCAP Searchback, based on payload text - or a snort rule!

All logs time-correlated with PCAPs and NetFlow V9 data

Unified web GUI, and a REST/API for workflow automation

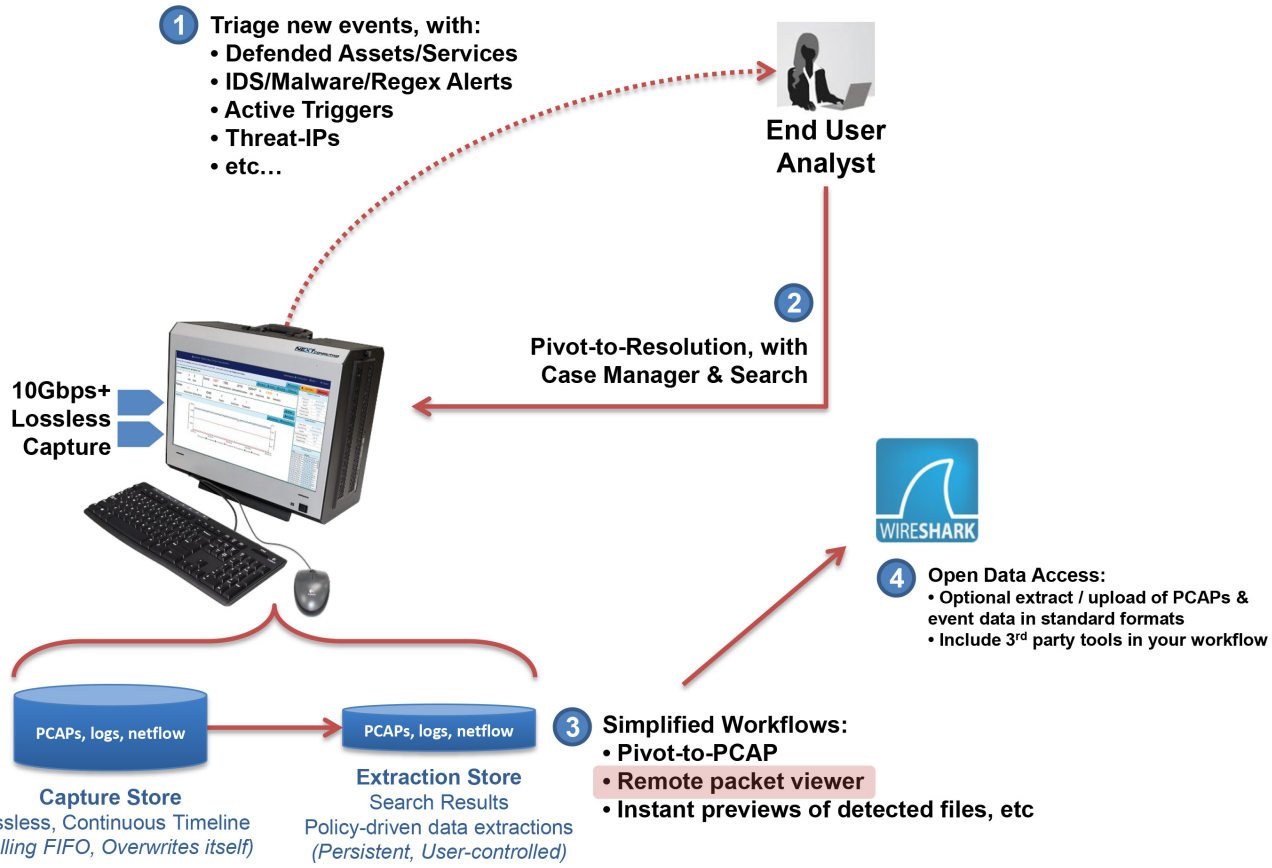
Manage reports & PCAPs for your entire cyber investigation

WEB GUI AND WORKFLOW FEATURES

- Define your own lists of Threat IPs & Trusted IPs
- One-click searching
  - Right click from a Critical Alerts Log, or a data graph.
- Remote access to streaming results
  - From a host-based WebGUI over the REST interface
  - From a streaming output port to any 3rd party forensics tool
- Stream initial search results to any visualization tool, even while a critical search is simultaneously running
- Visualization is pre-installed using open industry-standard data file formats:
  - PCAP & NetFlow V9 records open in WireShark
  - Log searches open as CSV files
  - Reports open as TXT/RTF files

Rev 2.5—3/20

CYBERPRO PLUS 100G WORKFLOW



CyberPro Plus 100G lets you jump quickly between PCAP actions and your tools-of-choice. Gain new insight from DPI analytics tools, and generate graphical incident reports. Then iterate new Active Trigger alerts and PCAP searches, to conclude your investigation quickly.

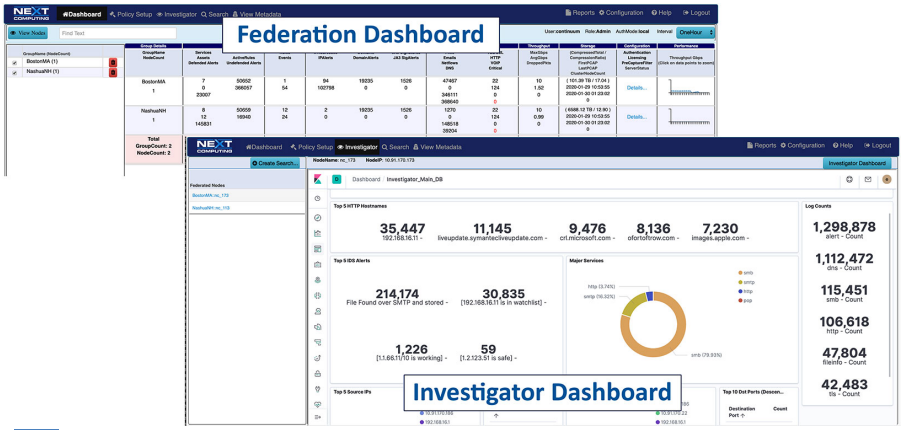
REAL-TIME ANALYTICS FEATURES

- Activate many simultaneous user-defined alerts: Snort/Suricata rulesets, ThreatIPs, BPF-based “Active Triggers”. Adjust them dynamically.
- Threat Hunting / Log Manager event options. All with search, cross-correlation and extraction:
  - HTTP
  - File event logging, with file size and URL or SMTP reference
  - DNS
  - Email
  - User agents
  - TLS/SSL
  - VOIP
  - Active Triggers (BPF signature)
  - Snort rule sets from pre-packaged or user-defined libraries
  - System events
- Flexible search actions:
  - All logs are time-correlated with PCAPs and NetFlow V9 data
  - Text search of logs, and text seachback of PCAP payload contentNetFlow V9 record logging and search
  - Search PCAP history, based on a SNORT/SURICATA ruleset
  - NetFlow V9 record logging and search
  - One-click searches auto-populate time period and search filter (BPF), based on context

NEXT COMPUTING

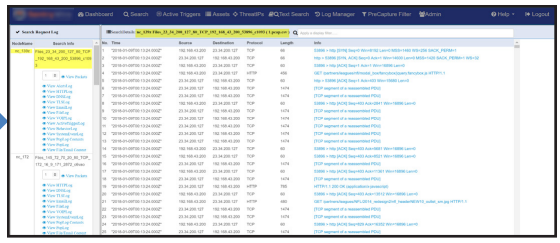
CyberPro Plus 100G

SITUATIONAL AWARENESS TOOLS VIA OPEN PCAP & OPEN IDS



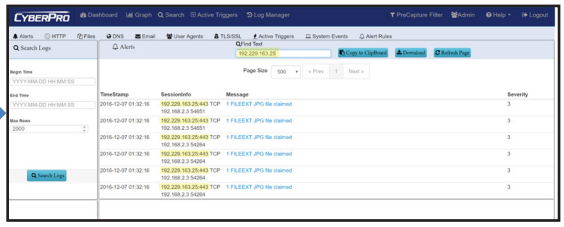
ANALYST OPERATIONS DASHBOARDS

- Prioritizes real-time Indicators of Compromise (IoC) & Incident Response actions
- Automated mapping of IoC events to adversary behavior in the Kill Chain
- One-click searches direct from the dashboard
- Live updates to the Capture Data Graph, and Critical Alerts List



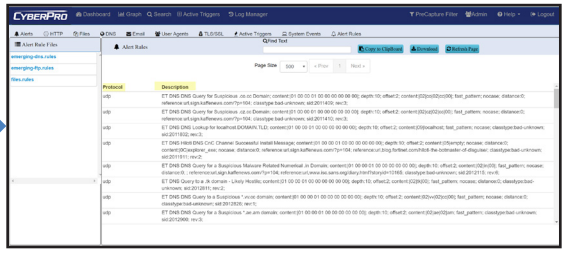
POLICY ALERTS DRIVES INCIDENT RESPONSE

- Start with red-flag behavior, like Exfiltration or suspect C&C activity
- One-click search to show IoCs for each step in the Kill Chain
- Then click to preview for all correlated PCAP data



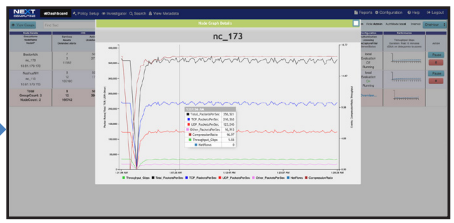
THREAT HUNTING / LOG MANAGER - IOC POLICIES

- SNORT/SURICATA Rule Sets
- Threat IPs
- Defended Assets & Services
- Active Triggers (BPF-based)
- Threat IPs and Suspicious Traffic alerts



THREAT HUNTING / LOG MANAGER - EVENT SEARCH ACTIONS

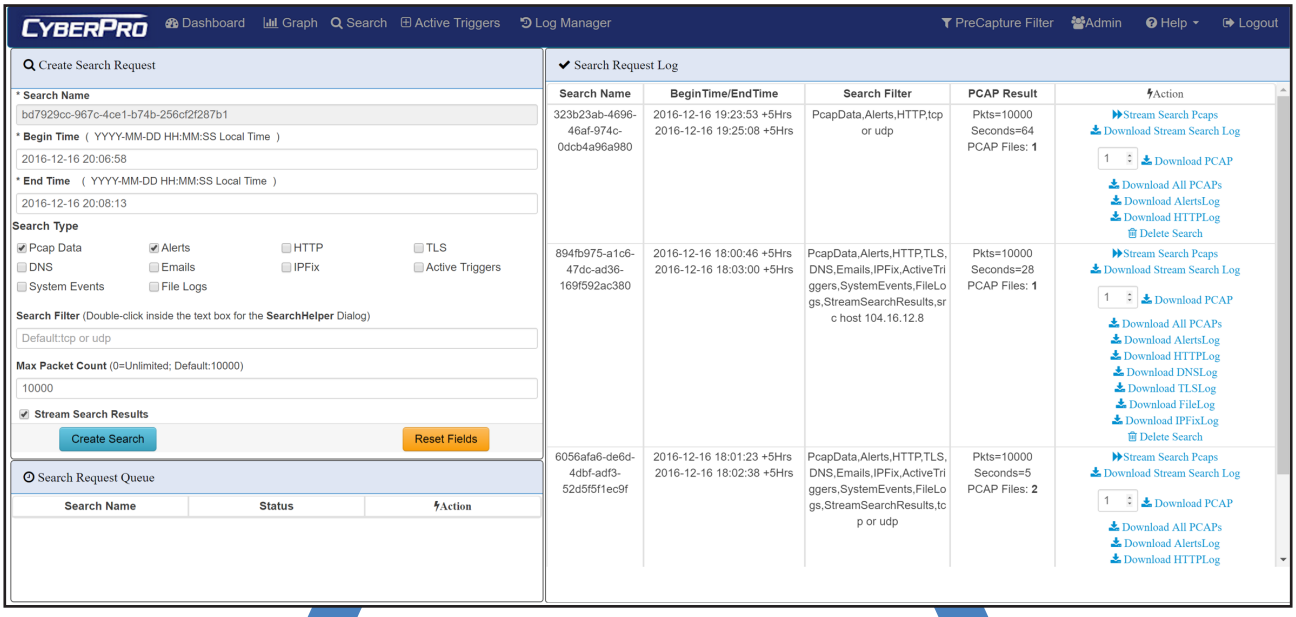
- One-click time-based BPF search
- Text-based search of alerts
- All IoC events correlated with PCAPs, NetFlow records, and sessionized logs



TIME-BASED DATA GRAPH

- With legends consisting of key packet capture and data compression statistics.
- One-Click search from any point in time, will automatically fill in a search request

SITUATIONAL AWARENESS TOOLS VIA OPEN PCAP & OPEN IDS

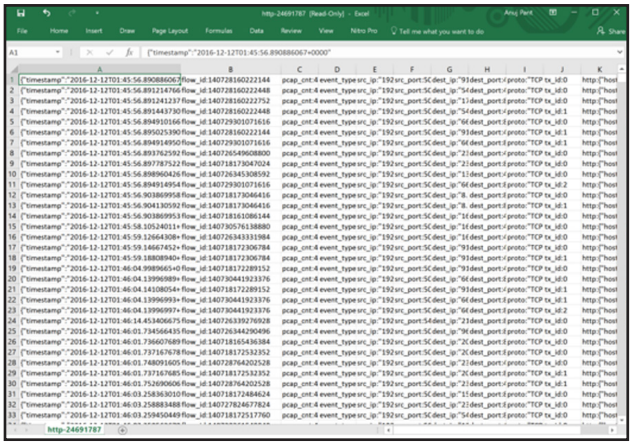


CYBERPRO PLUS 100G QUERY SCREEN

- Select time, filter and result data type(s)
  - Monitor and download results

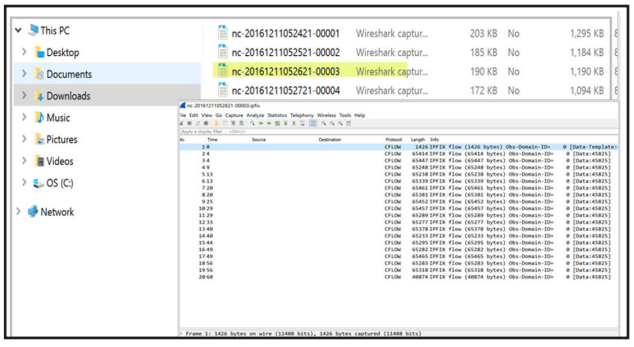
SEARCH/EXTRACT TO LOG FILES

eg. HTTP log data to Excel as CSV files

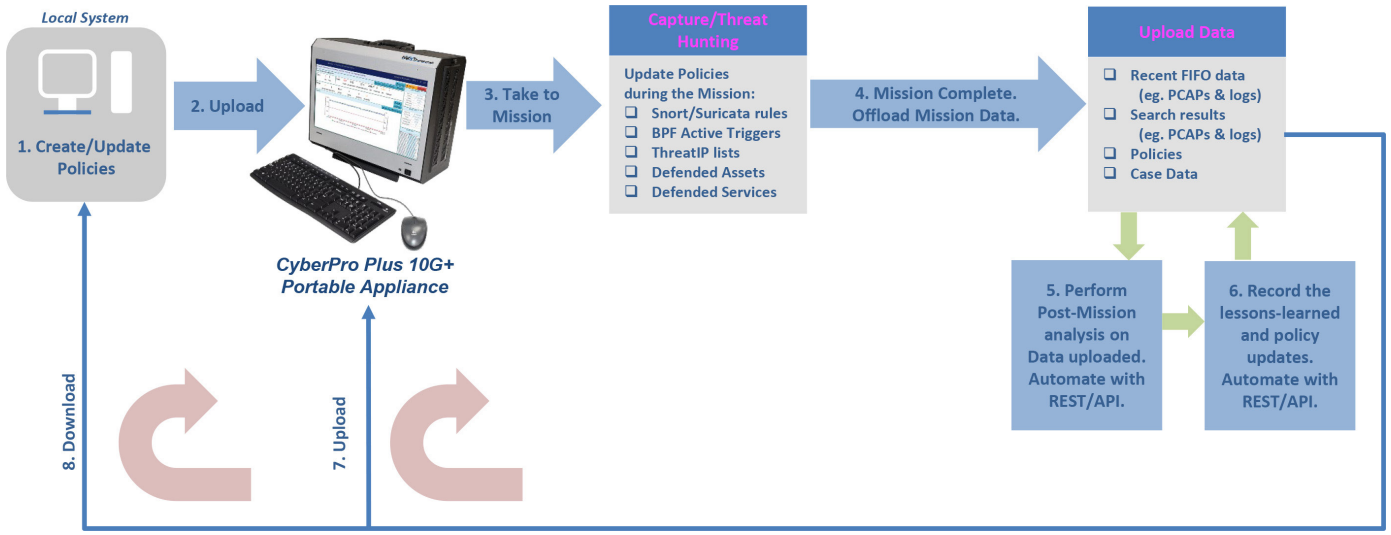


SEARCH/EXTRACT TO WIRESHARK

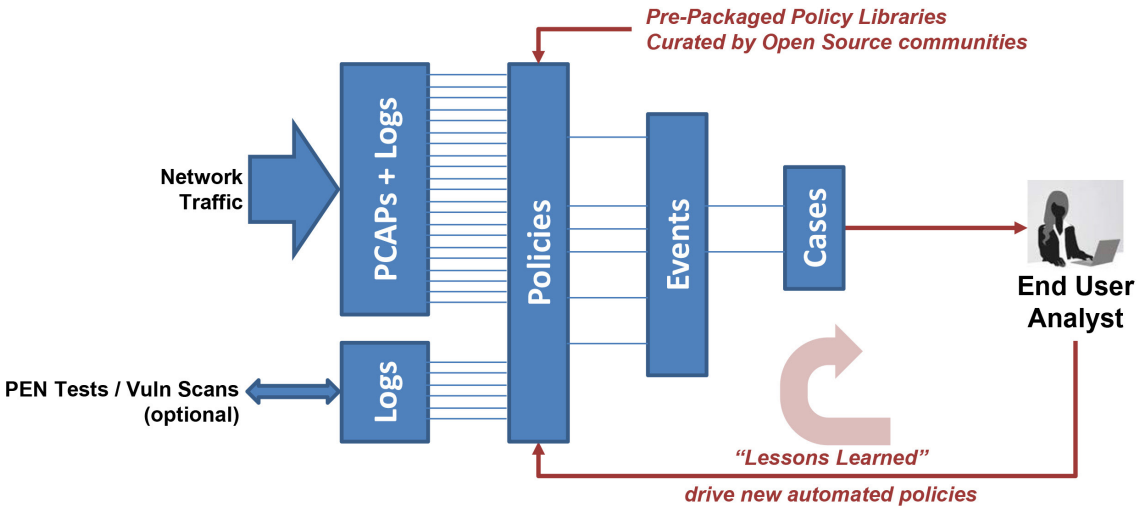
PCAP files or NetFlow V9 records



A PORTABLE CASE-MANAGEMENT FRAMEWORK



1. Cyber team will create/update initial policies on a local system.
2. Before each mission, upload these policies to a CyberPro Plus for use during the mission.
3. During the mission, Capture / Threat Hunting. Update real-time alerting policies, as required.
4. After the mission, offload data that includes marked case data, current policies, and last Capture Store / Extraction Store data.
5. Perform Post-Mission analysis on the data uploaded in step 4. Automate the post-mission analysis operations by utilizing the NextComputing REST/API.
6. Record the set of lessons learned and policy updates.
7. To iterate for the next mission, go to Step 2: upload and share new Policies with the CyberPro Plus appliance(s).
8. Download any updated policies to the local system, as needed to update and upload again.



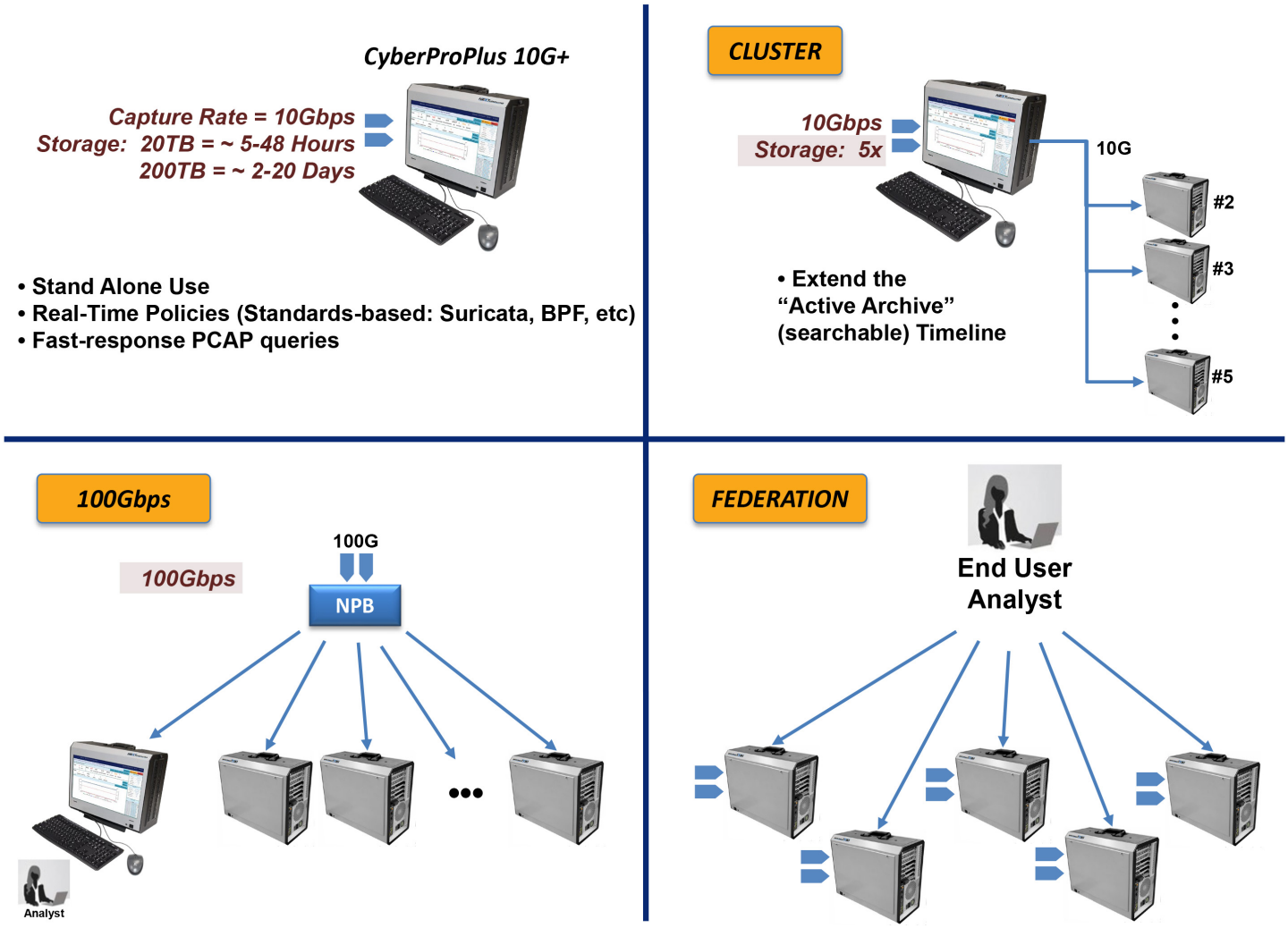
Integration on a small platform of Policy Management & Log Management & Forensics, provides the benefit "spiral model" of forensic investigations. Retain the lessons learned from prior missions, by provisioning new portables with the latest policy updates.

A PORTABLE BUILT FOR SCALE

When you require additional capture timeline in the field, configure and connect several other CyberPro Plus 100G appliances as “Cluster Nodes”. NextComputing’s unique MapReduce software framework spreads the processing load, so long timelines are as quick to search as with a single appliance.

When you set up multiple CyberPro Plus 100G appliances to capture at different locations, a single analyst use the Federation Manager capability for integrated remote access via unified web-based UI.

When you have ad-hoc requirements for lossless capture of very high capture rates, for 40Gbps, 100Gbps or even greater, the Federation Manager will also do the job. When high-rate traffic is split (using a Network Packet Broker or Load Balancer) into multiple 10G lines, each CyberPro Plus 100G can capture ip to 10Gbps+ of the load, and an end-user analyst will see all traffic integrated within the Federated UI. With Federation Manager features, it does not matter where the packets are located: You can make a single query for the whole traffic contents, and the results will be combined from all appliances into a single set of PCAP file results.

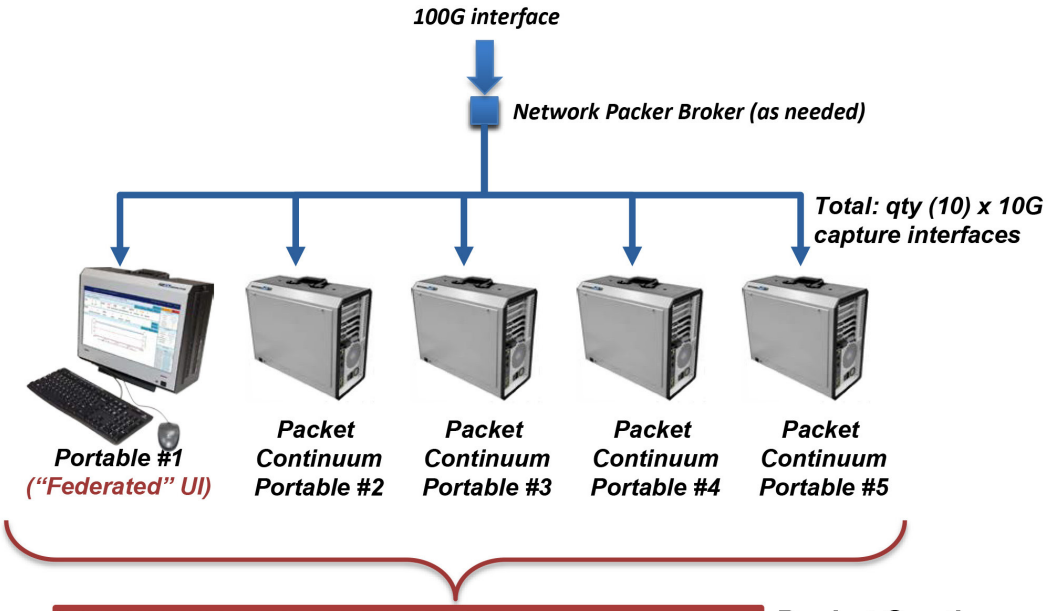


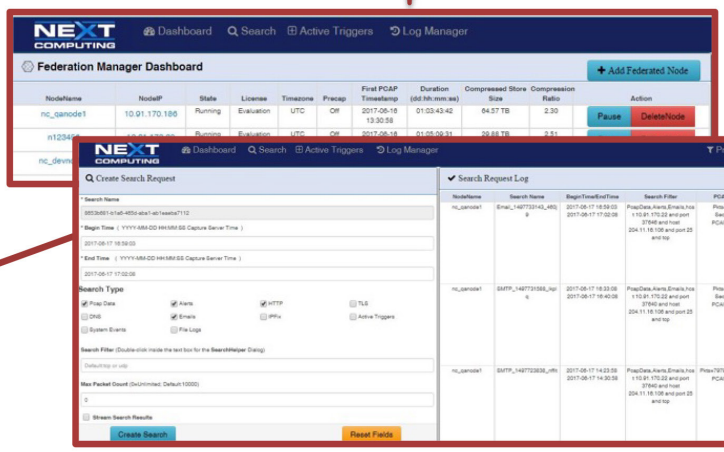
Rev 2.5—3/20

A PORTABLE BUILT FOR SCALE (continued)

Capture Rate:
100Gbps continuous lossless capture

Capture Timeline:
- ***33 hours, best case***
  - ***max compression***
  - ***70% usage***
- ***2.3 hours, worst case***
  - ***no compression***
  - ***100% bandwidth***
- ***100TB physical Capture Store***
  - ***= 5 x 20TB for each***



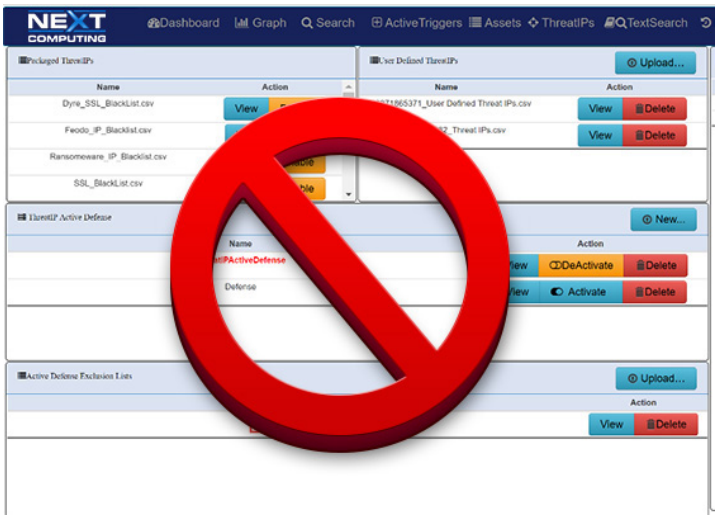


Packet Continuum "Federated" Local Display & WebGUI

File extraction & streaming replay output: Send PCAP query results into legacy 3rd party tools.

THREAT IP DETECTION

CyberPro Plus 100G enables identification, monitoring, viewing, and mitigation of pre-defined Threat IPs as well as user-defined IPs. The system comes pre-loaded with a known list of Threat IPs; a number of malicious IPs previously identified by trusted sources such as US-CERT, for your protection.



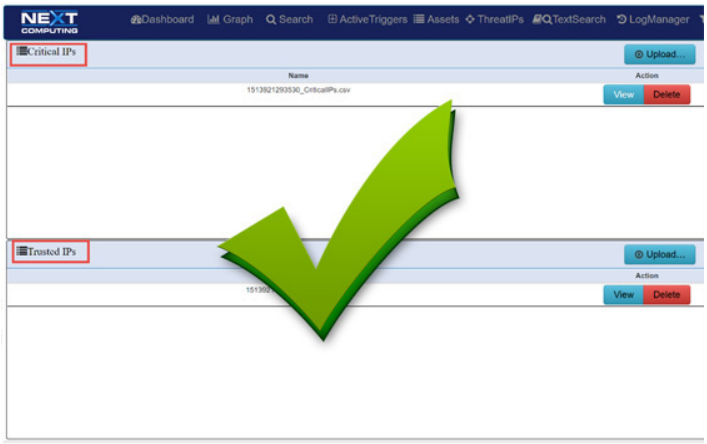
From the Threat Hunting / Log Manager or data graph, users can:

- Upload/enable, view or delete/disable lists of identified Threat IPs
- Set alerts based on identified Threat IPs
- Create Active Defense actions (via user criteria or Suricata rules) to be taken when a Threat IP is identified
- With one click, view detailed PCAP session information where a threat is identified

When a Threat IP is identified as present in a session, the system generates a severe alert and a pre-defined Active Defense action can be executed or, if one is not available, alert info can be sent to an external server.

DEFENDED ASSETS & SERVICES

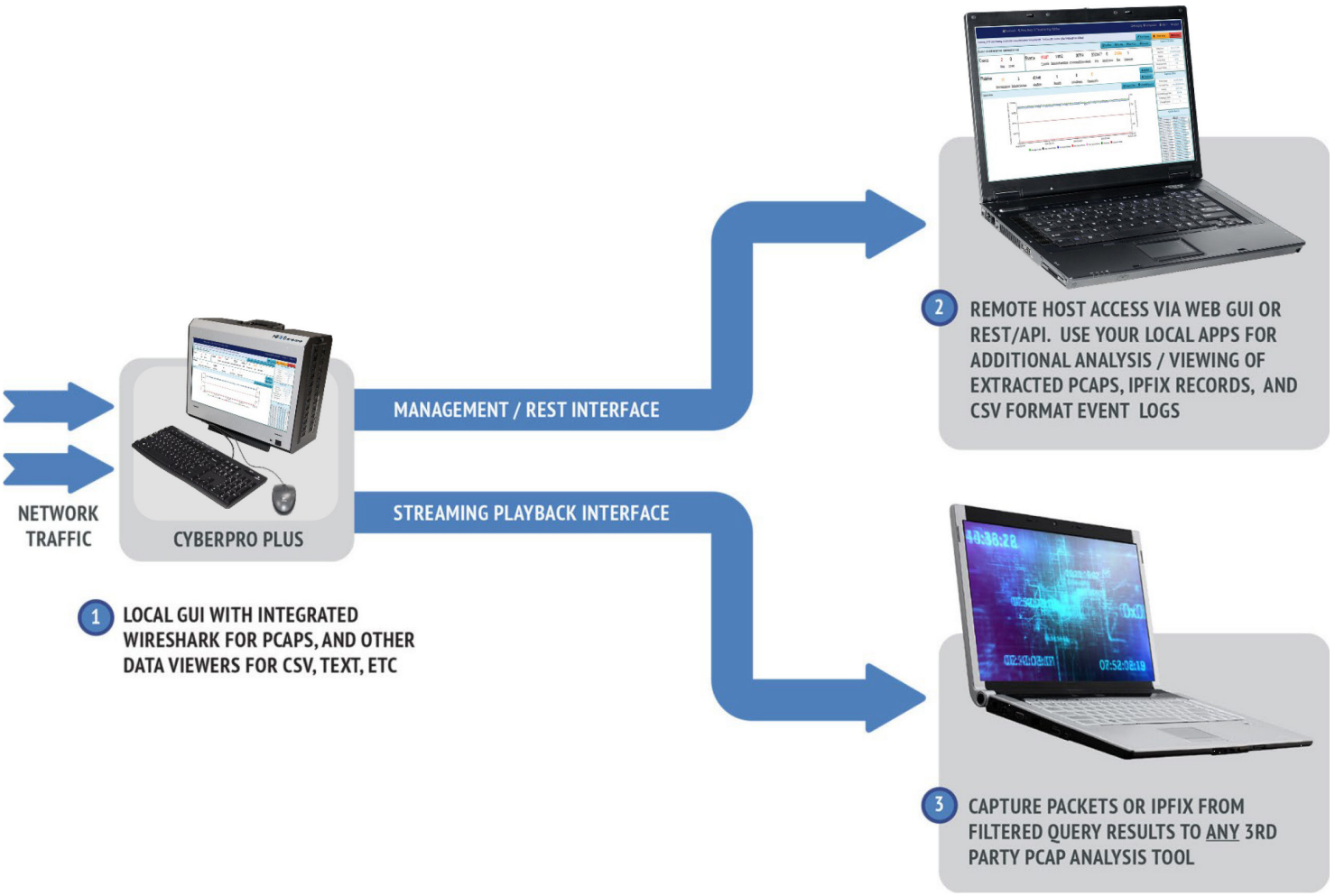
CyberPro Plus 100G enables identification, monitoring, viewing and automatic approval of Defended Assets, which consist of Critical IPs (essential infrastructure) as well as Trusted Asset IPs (host IP addresses defined as safe). Similarly, Defended Services for each critical network application/protocol are defined by port #.



Using the CyberPro Dashboard and Threat Hunting / Log Manager, users can:

- Upload, view or delete lists of identified Assets and Services
- Set alerts based on identified assets or services
- Monitor / view sessions containing specified assets/ services as the source or destination
- With one click from the dashboard, view detailed PCAP session information where an asset/service is identified

CyberPro Plus 100G OPEN DATA ACCESS



PACKET CAPTURE FEATURES

- Continuous lossless packet capture, with configurations supporting 10Gbps+, into a rolling FIFO Capture Store
- Searchable data recorder for NetFlow V9 netflow records and log files
- Real time indexing and alerting — with time stamping as low as 150 nanoseconds
- Data compression in real time — Overall storage amplification up to 5:1
- Dedicated onboard Extraction Store retains all search query results, retrievable by user-defined name
- Options for PCAP (or NetFlow V9) search results:
  - View in Wireshark on the local display UI
  - Remotely access from an external host via Web GUI or REST/API scripting
  - Run the critical sessions over the Streaming Playback Interface to any 3rd party forensic analysis tool. Simply connect streaming playback output to the capture interface of your tool, just like a span/mirror port.

TRANSPORTATION

SOFT CASE

- A high-quality, padded carrying bag is included with the CyberPro.
- Has room and extra pockets for your keyboard, mouse, cables, and other items
- The case can be branded with your logo stitched on the front
- Fits in the overhead bin on an airplane

FULL SIZE RUGGED CASE

- Full size rugged case with wheels and telescoping handle.
- Internal foam cutout snugly holds the CyberPro, as well as spaces for additional accessories
- Can be checked as baggage, while giving you peace of mind that your system is safe
- Exterior dimensions (L X W X D) – 24.60″ x 19.70″ x 11.70″ (62.5 x 50 x 29.7 cm)

RUGGED, SECURE HDD CASE

- Compact, lockable case for removable hard drives and SFP/SFP+ modules
- Holds up to (16) quick-time removable 2.5” drives AND
- Up to (8) SFP/SFP+ modules
- Internal security tray
- 16.44″ L x 13.00″ W x 6.82″ D (41.8 x 33 x 17.3 cm)

TSA COMPLIANT

- System with accessories and soft case is < 30lbs and small enough to be an airline carry-on
- Rugged case and system are < 50lbs, which can be checked as luggage without worry about damage.

Packet Capture Interfaces	10G fiber SFP+ SR and LR modules, 10G SFP+ copper, 1G RJ-45 copper SFP modules, 25G and 100G SFP28 SR and LR modules
Lossless Capture Rate	Rate Continuous lossless packet capture and enriched metadata generation, with configurations supporting 10Gbps-20Gbps+, into a rolling FIFO Capture Store or up to 100Gbps with PCAP capture only
Time Stamping Resolution	150 nanoseconds
IDS Alerts	Up to 50,000 dynamic Snort/Suricata rules (user-defined, or select from pre-packaged libraries)
ThreatIP alerts	Up to 1 Million dynamic IP Addresses (upload user-defined lists, or select from pre-packaged libraries)
Active Trigger Alerts	Up to 100 dynamic BPF-based Active Triggers (user-defined)
Log Manager: Actionable Search, All Time-Correlated with PCAPs and NetFlow Data	Real time logging/alerting: HTTP, files, DNS, email, user agents, TLS/SSL, VOIP, Active Triggers (BPF signature), system events, and Snort/Suricata IDS rules
NetFlow Record Logging (When Log Manager Analytics Enabled)	NetFlow V9 record logging in real time. Time line search of NetFlow V9 records. Extracted NetFlow V9 files viewable in WireShark
Local Display Data Viewers	For data extracted from search: PCAP and NetFlow V9 records in WireShark, all log files in spreadsheet viewer, and PCAP stream log viewable in text viewer. All extracted data can also be uploaded via the management port via remote browser-based Web GUI, or via REST API.
Remote Access	Remote access Web GUI access with same functionality as local display GUI, and remote access via REST/API. Both mechanisms allow off-load of PCAP, NetFlow V9 and log files from search into other 3rd party tools.
PCAP Playback Stream from Filtered Search	PCAPs filtered and extracted from search can be regenerated out a 1G copper RJ45 interface, like a span port, and can be directed to an external device for additional analytics, recording and signature analysis.

Capture Store (continuous rolling FIFO)	20TB, with options available for additional storage up to 200TB
Extraction Store (onboard storage for PCAP query results)	2TB (more with larger storage options)
Forensic Capture Timeline with 20TB Capture Store	
"Worst Case Timeline, with a 20TB Capture Store: No Compression, 10Gbps average (100% line rate)"	4.6 Hours
"Best Case Timeline, with a 20TB Capture Store: 5:1 Compression Ratio, 5Gbps average (50% line rate)"	2 Days
Forensic Capture Timeline, with a 200TB Capture Store	
"Worst Case Timeline, with a 200TB Capture Store: No Compression, 10Gbps average (100% line rate)"	2 Days
"Best Case Timeline, with a 200TB Capture Store: 5:1 Compression Ratio, 5Gbps average (50% line rate)"	20 Days

System	
Management Port	1G RJ-45 LAN port, to an external host for Web GUI and REST/API
Streaming Port	1G RJ-45 LAN port, to an external traffic/PCAP analyzer
Display	Integrated 17.3" LED LCD (1920x1080) for GUI and administration
Physical	• 7.09" (180.08mm) D x 16.78" (426.21mm) W x 14.16" (359.66mm) H (including folded-down handle) • <30 lbs, including a soft carrying case
Power	• 680W Gold Plus acoustically quiet PSU • Optional internal 460W/24V DC nominal (19V-36V DC range) power supply
Carrying Case	Soft case (included)
Optional Equipment	• International power cord • Telescoping-handle hard case • Large attaché-style hard case • "Lunchbox-size" hard case for accessory modules

4 Townsend West, Building 17, Nashua, NH 03063 • P: 1 (603) 886-3874 • F: 1 (603) 886-1736 • www.PacketContinuum.com • sales@Nextcomputing.com